Filtering [CL21]

$$x \in \mathbb{F}_p \longrightarrow \boxed{W} \longrightarrow \begin{cases} S \subset \mathbb{F}_p & \text{— } |S| \geq p-r+1 \\ S \ni x & \\ \text{or} & \\ \perp & \text{— "I don't know"} \end{cases}$$

$$\underbrace{|c * \hat{S}_1\rangle}\otimes \cdots \otimes |c * \hat{S}_n\rangle$$

$$\longrightarrow \boxed{(\Pi_i)_i} \longrightarrow \begin{cases} S \\ \text{or} \\ \perp \end{cases}$$

[CL21]
pick
the
POVM

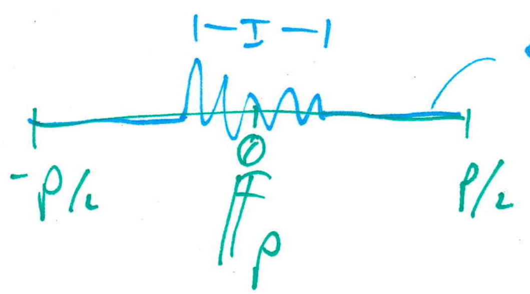
∃ simpler way to filter!
Change $|\hat{S}_i\rangle$

Free to choose

GET TO PICK THESE $\in \mathbb{C}$

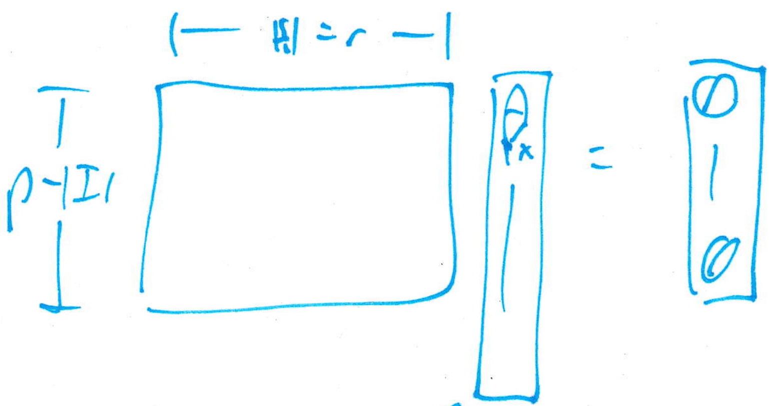
$$|\hat{S}_i\rangle = \sum_{x \in S_i} \beta_x |x\rangle$$

"preferred" symbols $\subsetneq \mathbb{F}_p$



$\langle y | \hat{S}_i \rangle = 0 \quad \forall y \notin I$

$\Rightarrow$ $p - |I|$ linear constraints on β_x's.



$\exists$ nonzero soln $\beta \in \mathbb{C}^r$ once $r \geq p+|I|+1$.

We get

$$\langle y \mid x * \hat{f}_i \rangle = 0 \quad \text{if } y \notin x + I.$$

ie, given y measured from $|x * \hat{f}_i\rangle$,

can infer $x \in \underbrace{y - I}_{\text{size} = |I| \geq p-r+1}$!

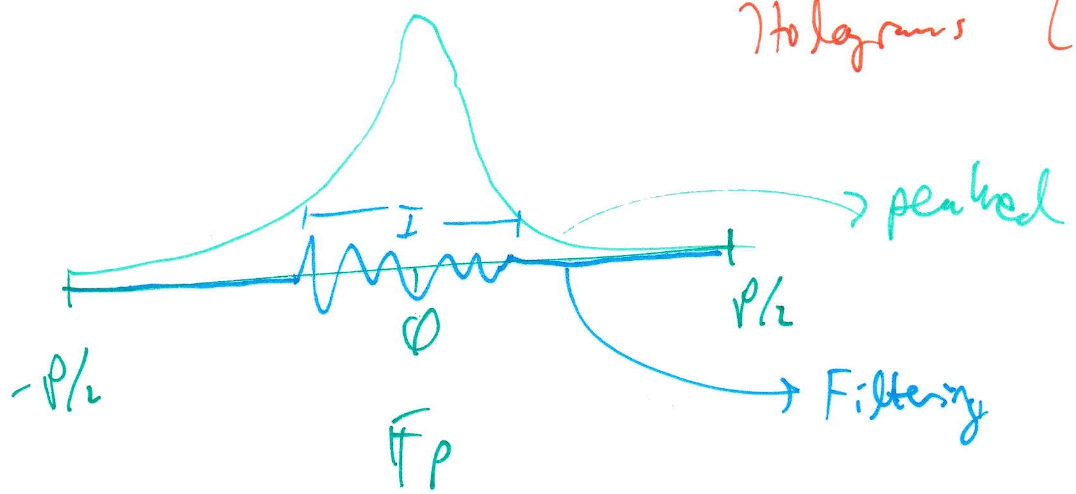
Succeeds with probability 1.

Still need expensive Arora-Ge Decoding...

"Error Holography"

proposed in [CT 24] for RS codes → Next Applications Concentration?

Holograms [implicit in [T24]]



Consider $\underset{x\sim|\hat{S}_i\rangle}{\mathbb{E}}\left[|x|^2\right] = \langle \hat{S}_i | D | \hat{S}_i \rangle$

$$D = \begin{pmatrix} (-p/2)^2 & & & \\ & (-p/2+1)^2 & & \\ & & \ddots & \\ & & & (p/2)^2 \end{pmatrix}$$

$$= \langle S_i | \hat{D} | S_i \rangle$$

$$= \beta^T \underbrace{\hat{D}\big|_{S_i \times S_i}}_{\text{submatrix}} \beta$$

Recipe: find β of smallest eigenvalue

$$\lambda_1\left(\hat{D}\big|_{S_i \times S_i}\right) = ?$$

Clearly,

$$\lambda_1\left(\hat{O}\,|_{S_i \times S_i}\right) \leq \mathrm{Var}[\quad]$$

$\vdash I \dashv$

$|I| \leq p-r+1$

$$\leq (p-r+1)^2$$

Aside: [CLZ21] solve the resulting polynomial system

$$\prod_{y \in [a_i, b_i]} (a_i \cdot x - y) = 0 \quad \forall i \in [m]$$

$c \in \mathcal{C}^\perp$
$\Rightarrow c = x^T A$ for some $x \in \mathbb{F}_p^n$

n variables, m eqns.
↳ degree ≥ 2 $= p - r + 1$

[Arora-Ge] - linearize eqns, solve w.h.p. once $m > \Omega(n^2)$

$\boxed{A}$

$m = \Omega = n^{p-r+1}$

Open Question: Can one do better?

[KS 99], [Courtois, et al 2000]
"relinearization"
related to Gröbner Bases...

Literature Review

standard paradigm: $|C\rangle \bigotimes_{i=1}^{m} \underbrace{|c_i * \hat{s}_i\rangle}$

Basis → info. about c_i → Classical Decoding Alg.

[YZ22, SJW+24 "DQI", CT24]	Computational Basis	Reed-Solomon Decoders
[CT23]	Unambiguous State Discrimination (USD) ↳ Sometimes learn c_i with certainty ☆	Gaussian Elimination
[CLZ21]	Filtering ↳ tells us $c_i \in S$ with certainty ☆	Arora-Ge

(non-chronological)

☆ Quantum Decoding Techniques

Codeword Holography

[CLZ21] • $m = n^{p \cdot n + 1} = \Omega(n^2)$

• Classical runtime $\Rightarrow 2^{\sqrt{m}}$ (prange)

• Uses filtering measurements

[CT23] • $m = \Theta(n)$

• Classical runtime poly(n) (prange)

• Uses USD measurements

[Now] • Relaxed problem

• $m = \Theta(n)$

• $2^{\sqrt{m}}$ prange runtime ~~vs poly n speedup~~

• Uses USD measurements ~~[illegible] sparsity of A.~~

In generality:

$c \sim \mathcal{C}^d$

$$c_i \to \boxed{\mathcal{N}_{\hat{\rho}_i}} \to |c_i * \hat{\rho}_i\rangle \to \boxed{(\Pi_i)} \to X \in [M]$$

classical channel

$$c_i \to \boxed{W} \to X_i$$

① Can pick any $|\hat{\rho}_i\rangle$ s.t. $\langle \rho_i | f_i | \rho_i \rangle \geq \alpha$

② Can pick $(\Pi_i)_{i=1}^{M}$ to be ANY POVM

Open Question: How can we maximize, e.g.

$$I(c_i, X_i)$$

Chailloux & Tillich 23: USD POVM

$$c_i \to \boxed{W} \to \begin{cases} c_i & \text{w.p. } 1-p_\perp \\ \perp & \text{w.p. } p_\perp \end{cases}$$

Unambiguous
State
Discrimination

Set $|\psi_1\rangle - |\psi_p\rangle \in \mathbb{C}^p$

Define $G_{ij} = \langle \psi_i | \psi_j \rangle$

Thm: $\lambda_1(G) \leq 1 - p_\perp$ for some USD povm

2-3pm Noah's Talk

3pm Tea

SKIP

proof (skip)

Assume WLOG $\lambda_1 := \lambda_{min}(G) > \emptyset$.

Define $|\bar{\Psi}_i\rangle$ so that $\underbrace{\langle\bar{\Psi}_i|\Psi_j\rangle = \delta_{ij}}_{\text{i.e., } \bar{\Psi}^\dagger \Psi = I}$.

$\bar{\Psi} := [\,|\bar{\Psi}_1\rangle \text{ —— } |\bar{\Psi}_p\rangle\,]$.

Notice that $\bar{\Psi} = \Psi G^{-1}$ as

$$\bar{\Psi}^\dagger \Psi = (G^{-1})^\dagger \Psi^\dagger \Psi = G^{-1} G = I.$$

Use as POVM operators: $\alpha_i |\bar{\Psi}_i\rangle\langle\bar{\Psi}_i|$ for some α_i s.t. $\underbrace{\sum_{i=1}^{p} \alpha_i |\bar{\Psi}_i\rangle\langle\bar{\Psi}_i| \leq I}$.

~~Key~~ just need to show that this is the case

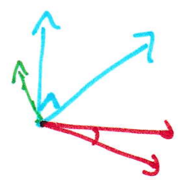
ACTUALLY: $\lambda_1 = \alpha_i$

$\{\lambda_1 |\bar{\Psi}_i\rangle\langle\bar{\Psi}_i|\}$ is a POVM

So, we have

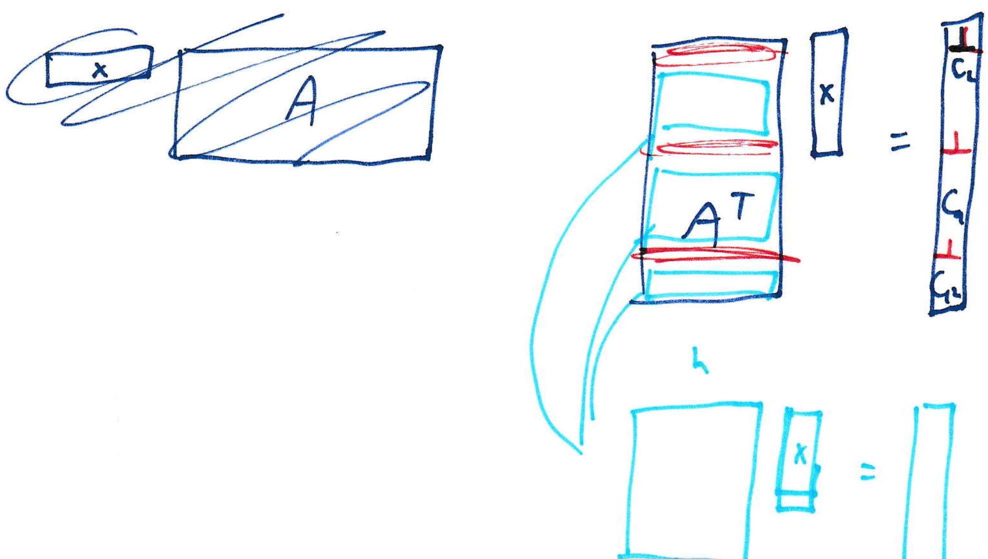
$$\mathbb{P}[\text{successful USD}] \geq \lambda_1(G)\,!$$

Intuitive picture:



$$\xi\ \underbrace{|c_1 * \hat{\zeta}_1\rangle}_{\to\, c_1 \text{ or } \perp} \otimes \underbrace{|c_2 * \hat{\zeta}_2\rangle}_{\to\, c_2 \text{ or } \perp} \otimes \cdots \otimes \underbrace{|c_m * \hat{\zeta}_m\rangle}_{\to\, c_m \text{ or } \perp}$$

Erasure Decoding!



if this is FULL RANK(h) we can determine x uniquely! (e.g., using Gaussian Elimination)

What is $\lambda_1(G)$ if $|\psi_x\rangle = |x * \hat{g}_i\rangle$?

$$|g_i\rangle = \sum_{x \in \mathbb{F}_p} \beta_x |x\rangle \quad \text{s.t.} \quad \langle g_i | f_i | g_i \rangle = \alpha$$

$$G_{xy} = \langle x * \hat{g}_i \underset{QFT^\dagger QFT}{|} y * \hat{g}_i \rangle$$

$$= \langle \hat{x} \times g_i | \hat{y} \times g_i \rangle$$

$$= \underbrace{\sum_{z \in \mathbb{F}_p} \omega_p^{(y-x)z} |\beta_z|^2}_{\text{circulant}}$$

$$G_{xy} = \text{fn of } y - x$$

exercise:
$$\hat{G} = \begin{pmatrix} p \cdot |\beta_0|^2 & & \\ & \ddots & \\ & & p \cdot |\beta_{p-1}|^2 \end{pmatrix}$$

$$\Rightarrow \lambda_1(G) = \lambda_1(\hat{G}) = p \cdot \min_{x \in \mathbb{F}_p} |\beta_x|^2$$

$$|\xi_i\rangle = \sum_{x \in f_i^{-1}(1)} \beta_x |x\rangle + \sum_{x \notin f_i^{-1}(1)} \beta_x |x\rangle$$

$$\sum |\beta_x|^2 \geq \alpha \qquad \sum |\beta_x|^2 \leq 1-\alpha$$

$\Rightarrow \exists\, x \in f_i^{-1}(\emptyset)$

s.t. $|\beta_x|^2 \leq \dfrac{1-\alpha}{|f_i^{-1}(\emptyset)|} = \dfrac{1-\alpha}{p-r}$

$r = |f_i^{-1}(1)|$

So $\lambda_1 \leq \dfrac{1-\alpha}{p-r} \cdot p$!

[Chefles, Barnett 1998]: λ_1 is optimal in this case

$$\lambda_1 = \max_{\text{povms}} (1 - P_\perp)$$

For erasure decoding of $\mathcal{C}^\perp$ w.h.p.

need $p_\perp \le 1 - \frac{h}{m}$. $\iff$ $1 - p_\perp \ge \frac{h}{m}$

But we know that $\lambda_1 \le \frac{1-\alpha}{p-r} \cdot p$

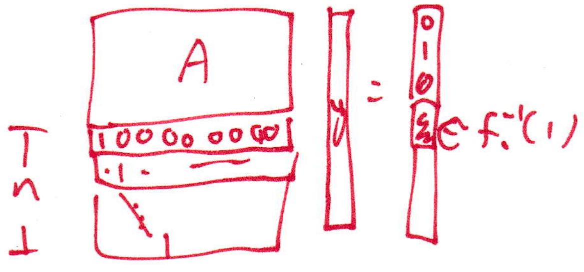
$$\lambda_1 = \text{best } 1 - p_\perp .$$

So $\frac{h}{m} \le \frac{1-\alpha}{p-r} \cdot p$

$$\left(1 - \frac{r}{p}\right) \cdot \frac{h}{m} \le 1 - \alpha$$

$$\Rightarrow \alpha \le 1 - \frac{h}{m} + \frac{h}{m} \cdot \frac{r}{p}$$

Prange's Alg.



$$\langle \textstyle\sum_i f_i \rangle = n + (m-n) \cdot \frac{r}{p}$$

$$\langle \textstyle\sum_i f_i \rangle / m = 1 - \frac{h}{m} + \frac{h}{m} \cdot \frac{r}{p}$$

$$\Rightarrow \alpha_{prange} \ge \alpha_{USO}$$

Not obvious how to get Q. advantage from USO

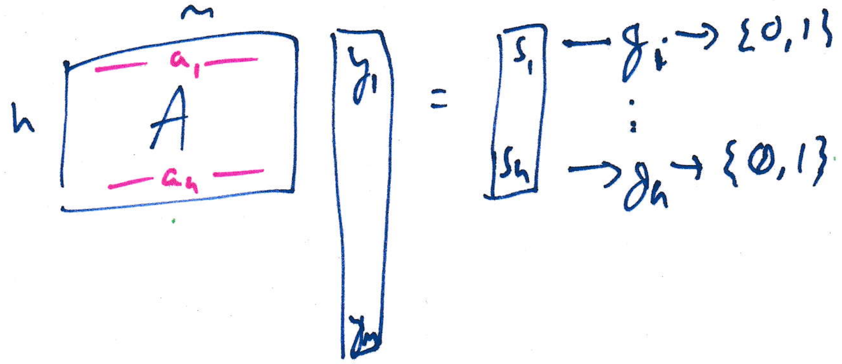
One big open question:

Can we get exponential speedup using

USD decoding?

Variants of LINSAT?

Holography?

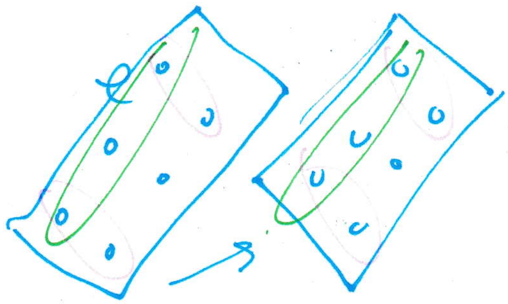


Define $\mathcal{C}^g$ as $\{y \in \mathbb{F}_p^m : g_i(a_i \cdot y) = 1 \ \forall i \in [n]\}$

Let $t = |g_i^{-1}(1)|$.

Set $t = p - p^a$ for some $a < 1$

$m = \Theta(n) = \Theta(p^b)$



Need a random string $y \sim \mathbb{F}_p^m$ to be $y \notin \mathcal{C}^g$ w.h.p.

$$\frac{|\mathcal{C}^g|}{|\mathbb{F}_p^m|} = \left(\frac{p - p^a}{p}\right)^n = \left(1 - \frac{1}{p^{1-a}}\right)^{p^b}$$

$$= \left(1/e\right)^{p^{a+b-1}}$$

$=$ small if $a + b > 1$.

$$|e^g\rangle = \sum_{s\in g^{-1}(1)} \beta_s \sum_{Ay=s} |y\rangle$$

Codeword Holography: set β_s to shape $|\hat{e}^g\rangle = ?$

$$y(s) = \prod_{i=1}^{h} y_i(s_i)$$

$$|e^g\rangle = \left|\left(\sum_{s_1\in g_1^{-1}(1)} \beta^{(1)}_{s_1} \sum_{\substack{y\in \mathbb{F}_p^n \\ a_1\cdot y = s_1}} |y\rangle\right) \times \cdots \times \text{"} \quad \text{"}\right\rangle$$

$$|\hat{e}^g\rangle = \left|\bigotimes_{i=1}^{h} \sum_{s_i\in g_i^{-1}(1)} \beta^{(i)}_{s_i} \sum_{x\in \mathbb{F}_p} \omega_p^{xs_i} |x\cdot a_i\rangle\right\rangle$$

$$\begin{array}{cc} & s \rightarrow \\ I \ni x \downarrow & \begin{bmatrix} \omega_p^{sx} \end{bmatrix} \end{array} \begin{bmatrix} \beta^{(i)} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

need $p - |I| < t = p - p^a$

Holography is same as before!

filter scalars to I of size $p - |g_i^{-1}(1)| + 1$
$\sim p^a$

So we receive $c_i = \sum_{j=1}^{h} A_{ji} \cdot x_j$ where

each $x_j \in [-p^a/2, p^a/2]$.

If $A_{ij} \in [-K, K]$,

then $$\mathrm{Var}(c_i) \sim h \cdot \mathrm{Var}(x_j) \cdot K^2$$
$$\sim p^b \cdot (p^a K)^2$$

$$\Rightarrow \forall \epsilon > 0$$

$$\mathbb{P}[|c_i| > p^{b/2+a+\epsilon} \cdot K] = o(1/p)$$

If $\frac{b}{2} + a < 1$, this confines c_i to a vanishing fraction of $\mathbb{F}_p$, enabling LWO.

But what if we use

$$\mathrm{Var}[\Omega] = \lambda_1(\hat{D}|_{S_i})?$$

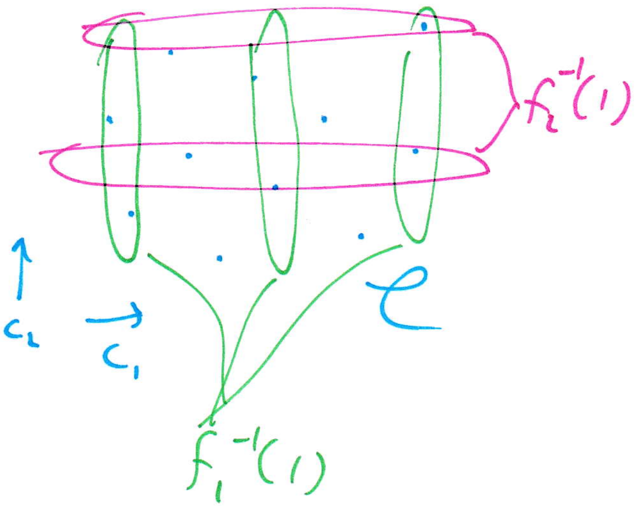
I Background

$\mathcal{C} \subseteq \mathbb{F}_p^m$ linear code, p prime

$$\mathcal{C} = \{ Bx : x \in \mathbb{F}_p^n \} = \{ y \in \mathbb{F}_p^m : Ay = 0 \}$$

$$\begin{array}{cc} & n \\ m & \boxed{B} \end{array} \qquad \begin{array}{cc} & m \\ h & \boxed{A} \end{array} \qquad h + n = m$$

$\mathcal{C}^\perp = \ker B^T =$ "swap $A \leftarrow B^T$, $B \leftarrow A^T$"



$c_1 - f_1 \to \{0,1\}$

$c_2 - f_2 \to \{0,1\}$

$\vdots$

$c_m - f_m \to \{0,1\}$

Max-LINSAT: output $c \in \mathcal{C}$ s.t. $\sum_i f_i(c_i) \geq \alpha \cdot m$

$\alpha = 1 \Rightarrow$ LINSAT

$$r := |f_i^{-1}(1)|$$

$$1 \leq r < p$$

Why solve (max-) LINSAT?

2 reasons:

① max-CUT → NP-hard to solve exactly

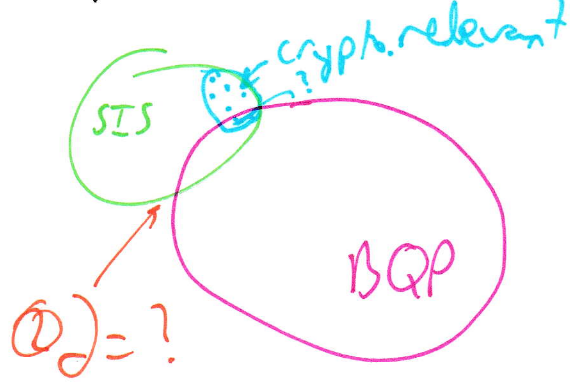
$\Downarrow$ generalization

max-LINSAT

$\Uparrow$

② SIS_∞ – short integer solutions

problem space



Regev's approach

$$|\mathcal{C}\rangle = \sum_{c \in \mathcal{C}} |c\rangle \longrightarrow \boxed{\text{Regev}} \longrightarrow |\mathcal{C} \times \mathcal{S}\rangle$$

$$|\mathcal{S}\rangle = |\mathcal{S}_1\rangle \otimes \cdots \otimes |\mathcal{S}_m\rangle$$

$$\mathbb{E}_{x \sim |\langle \mathcal{S}_i | x\rangle|^2}\left[f_i(x)\right] = \langle \mathcal{S}_i | f_i | \mathcal{S}_i\rangle = \alpha \in [0, 1]$$

$$|\mathcal{C}\rangle|\mathcal{S}\rangle \xrightarrow{\text{Regev}} \underline{|\mathcal{C} \times \mathcal{S}\rangle}|0\rangle$$

if $|\psi\rangle = \sum_x \psi_x |x\rangle$ . . .

$$|\psi \times \phi\rangle := \sum_x \psi_x \phi_x |x\rangle$$ "pointwise product"

Recall, $\mathrm{QFT}|x\rangle = |\hat{x}\rangle = \frac{1}{\sqrt{q}} \sum_{y \in \mathbb{F}_q} \omega_q^{xy} |y\rangle$.

Theorem: $\forall \psi, \phi$

$$|\psi * \phi\rangle := \sum_{x,y} \psi_x \phi_y |x+y\rangle = \mathrm{QFT}^\dagger |\hat{\psi} \times \hat{\phi}\rangle$$

Recipe for $|\mathcal{C} \times \mathcal{S}\rangle$:

1) prepare $|\mathcal{C}\rangle|\mathcal{S}\rangle$

2) QFT $\rightarrow |\hat{\mathcal{C}}\rangle|\hat{\mathcal{S}}\rangle$

3) Reversible Convolution: $\longrightarrow |\hat{\mathcal{C}} * \hat{\mathcal{S}}\rangle|0\rangle$

4) $QFT^{\dagger}$ $\longrightarrow \underbrace{|\mathcal{C} \times \mathcal{S}\rangle}$

$\hookrightarrow$ measure, get $c \in \mathcal{C}$

$\langle \mathcal{C}\times\mathcal{S}| \sum_i f_i |\mathcal{C}\times\mathcal{S}\rangle \approx \alpha \cdot n$

What is $QFT|\mathcal{C}\rangle$?

<u>Claim</u>: $QFT|\mathcal{C}\rangle = |\mathcal{C}^\perp\rangle$.

<u>proof</u>: First, consider $\underline{QFT|\ker a_i^T\rangle}$.

where $A = \begin{bmatrix} — a_1^T — \\ \vdots \\ — a_n^T — \end{bmatrix}$. What is THAT?

$\cancel{\sum \alpha \cdot a_i}$ Well, it's just $\sum_{x \in \mathbb{F}_p} |x \cdot a_i\rangle$

Because $QFT \cdot \sum_x |x \cdot a_i\rangle$

$$= \sum_{z,x} \omega_p^{x \cdot z^T a_i} |z\rangle$$

If $z^T a_i = 0$, $\sum_x \omega_p^{x \cdot (z^T a_i)} = p$

If $z^T a_i \neq 0$, $\sum_x \omega_p^{x \cdot (z^T a_i)} = 0$ by symmetry.

$$\Rightarrow \alpha \sum_{y^T a_i = 0} |y\rangle = |\ker a_i^T\rangle.$$

By the convolution Theorem,

$$QFT|\mathcal{C}\rangle = QFT|\ker a_1^T \times \cdots \times \ker a_n^T\rangle$$

$$= |\widehat{\ker a_1^T} * \widehat{\ker a_2^T} * \cdots * \widehat{\ker a_n^T}\rangle$$

$$= \sum_{x_i} |x_1 \cdot a_1 + \cdots + x_n \cdot a_n\rangle = |\mathcal{C}^\perp\rangle \quad \square$$

$|\hat{f}\rangle = ?$

$= |\hat{f}_1\rangle \otimes \cdots \otimes |\hat{f}_n\rangle$

Limiting Cases

1) No constraint: $|f_i\rangle = \sum_{x\in\mathbb{F}_p} |x\rangle \Rightarrow |\hat{f}_i\rangle = |0\rangle$

2) Strictest: $|f_i\rangle = |x\rangle \Rightarrow |\hat{f}_i\rangle = \sum_{y\in\mathbb{F}_p} \omega_p^{x\cdot y}|y\rangle$

$$|\hat{e}\rangle|\hat{f}\rangle \rightarrow |\hat{e} * \hat{f}\rangle|0\rangle$$

$$\sum_{c\in\mathcal{C}^\perp} |c\rangle|\hat{f}\rangle \rightarrow \sum_{c\in\mathcal{C}^\perp} |c\rangle \underbrace{|c * \hat{f}\rangle}_{\substack{\text{un-"decode c"} \\ \text{uncompute}}} \rightarrow |0\rangle \sum_{c\in\mathcal{C}^\perp} |c * \hat{f}\rangle$$

$$= |\hat{e} * \hat{f}\rangle$$

II methods

$$|0\rangle \bigotimes_{i=1}^{m} \underbrace{|c_i * \hat{\xi}_i\rangle}_{} \xrightarrow{Dec} |c\rangle \hat{\bigotimes_{i=1}} |c_i * \hat{\xi}_i\rangle$$

1. "measure" in some "basis"
2. Classically decode c

Defn: A M-outcome POVM over $\mathbb{C}^p$ is a tuple

$$(\Pi_1, \ldots, \Pi_M)$$

$$\Pi_i \in \mathbb{C}^{p \times p}$$

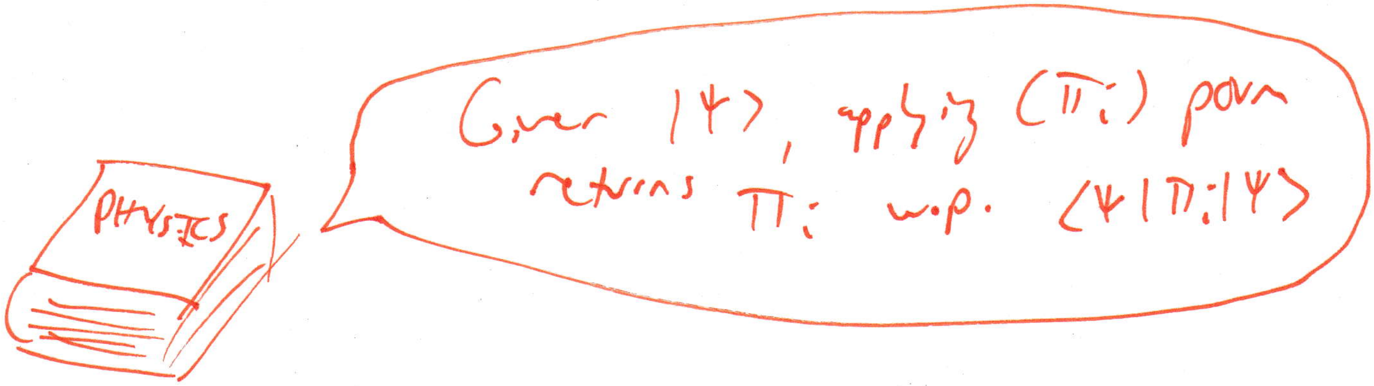
(i) Hermitian $\Pi_i^{\dagger} = \Pi_i$

$\Rightarrow$ real eigenvalues

(ii) $\sum_{i=1}^{M} \Pi_i = I$

(iii) $\Pi_i \succeq 0$ ie $\lambda_1(\Pi_i) \geq 0 \ \forall i$

"smallest eigenvalue"



Ex: min-error measurement given $|c_i * \hat{s}_i\rangle$
$c \in \mathbb{F}_p$

$(\Pi_1 - \Pi_p)$

$\Pi_x \Rightarrow$ "c_i is probably $= x$"

wrong with probability

$$P_{error} = \frac{1}{p} \sum_{y \neq x} \langle y * \hat{s}_i | \Pi_x | y * \hat{s}_i \rangle$$

= linear in entries of Π_x

Can minimize (or maximize) Perror by solving SDP

$(\Pi_x \succeq 0)$